SOC rendszerek fejlesztése az AI korszakában

Sajó Péter

InfoSec Üzletág Igazgató, EURO ONE Zrt.

2026. 03. 04.

Business & Security

EURO ONE INFOSEC Üzletág

- 20 év tapasztalat
- 50+ szakértő
- Kiemelkedő hazai és nemzetközi referenciák
- Hálózat, ITSec, SIEM/SOC , GRC, Automatizálási tudás
- SOC érettség felmérés, Purple team gyakorlatok, SOC roadmap tanácsadás, stb.
- Menedzselt SOC szolgáltatás itthon és külföldön (ISO 27001 minősítéssel)

EURO ONE Számítástechnikai Zrt. 1145 Budapest, Újvilág u. 50-52
www.euroone.hu | info@euroone.hu | +36 1 358 6350

euro one

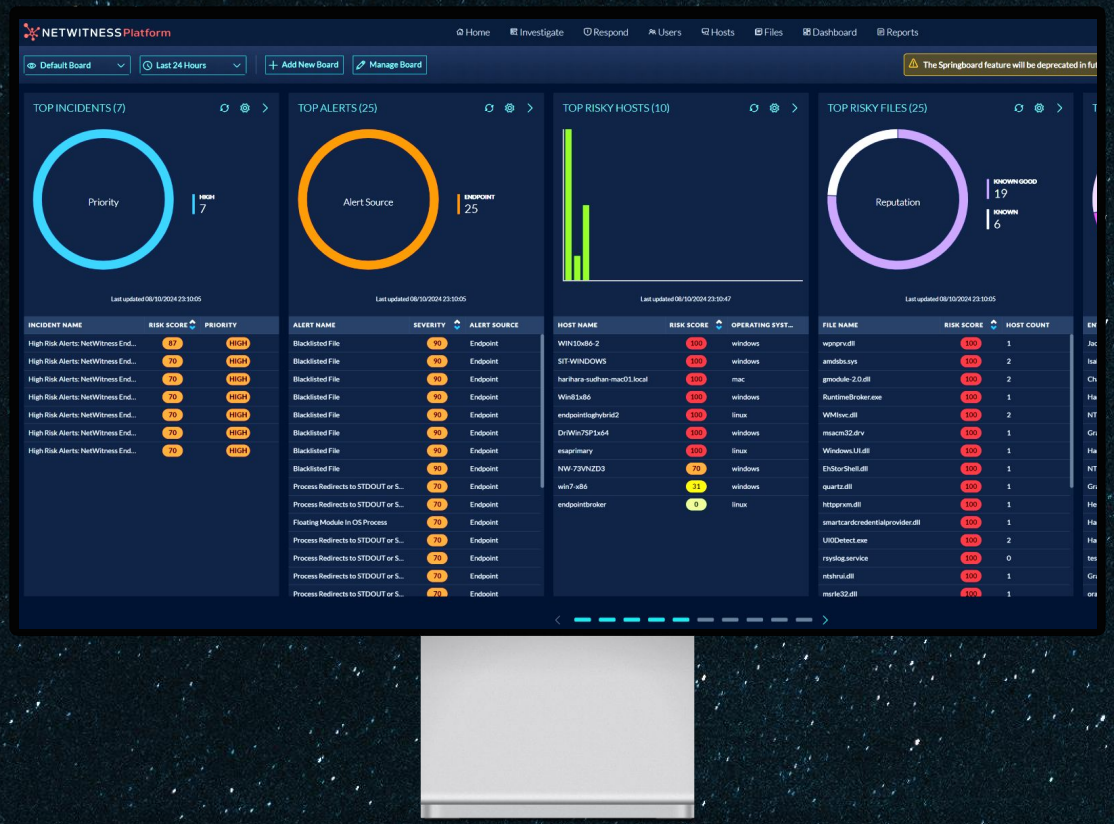
Mi is az a SOC (Security Operations Center)?

Based on NIST CSF

- SOC ≠ Technology
- SOC ≠ Process
- **SOC = PPP**
  (People + Processes + Technology)

Jelenlegi SOC kihívások #1

- AI alapú támadások
- 40+ technológia, melyek sokszor átfedésben vannak
- Nagy mennyiségű adat, hosszú megőrzési idők
- Go to Cloud nyomás
- A SIEM rendszer szabályrendszerének lassú fejlesztése és karbantartása
- Lassú és költséges automatizálás



Jelenlegi SOC kihívások #2

- Túl sok riasztás, incidens
- Túl sok false pozitív riasztás
- Lassú elemzés és reagálás
- Gyorsan kiégő elemzők
- Folyamatos HR problémák
  (keresés – betanítás – motiválás - megtartás)
- A SOC folyamatok fejletlensége
- Egymással küzdő ITSec és IT üzemeltetési csapatok
- Hiányzó kapcsolat a kockázatok és az ITSec események között
- Hiányzó kritikus szerepkörök (Threat Hunting, CTI processing)
- Hiányzó 7x24 szolgáltatás
- Folyamatos költségcsökkentési nyomás

Vízió: Autonom SOC

A SOC fejlődése

Reactive SOC

Perception

Automated SOC

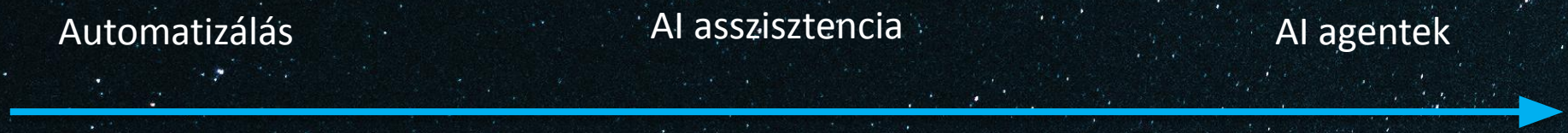
Responsive

Learinging

Perdictive SOC
AI based SOC

Forcasting

Az autonom SOC alapja - AI



Automatikusan lefutó, előre lefejlesztett folyamatok

Az AI válaszokat ad a kérdésekre, összefoglal, begyűjt, javasol prompt formájában

Teljes szerepkörök átvétele, autonom munkavégzés ‚Human-in-the loop' kontroll mellett

ML/SOAR

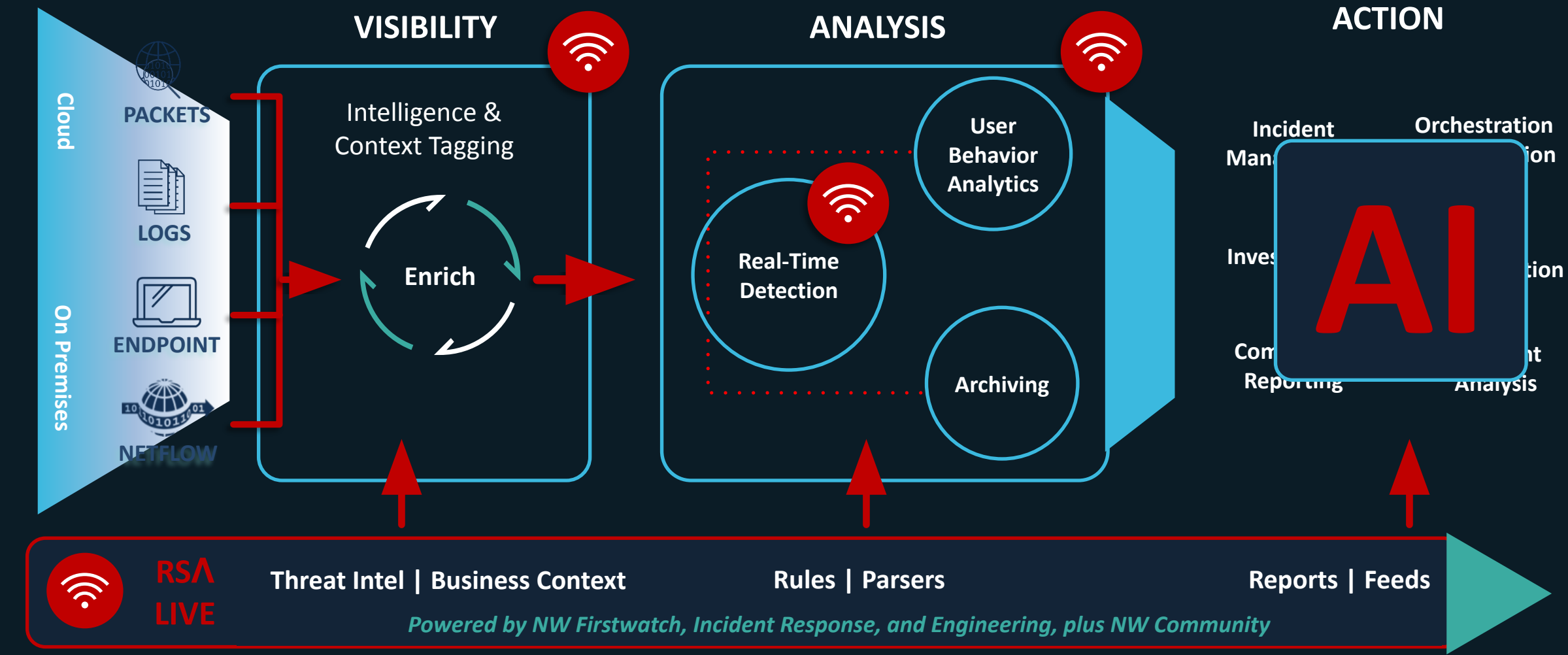
LLM

Agentic AI


euro one
NetWitness AI Analyst
The agentic AI platform
AI-powered SOC augmentation for faster, more accurate incident response

Netwitness Agentic AI platform

- Agentic AI ecosystem
- On-prem NW data lake alapokon
- Beépített ML/AI előszűrő rendszer utáni réteg
- Minimális felhős kitettség
- Teljes szerepkör ellátás
- Egymással összedolgozó, moduláris rendszer


VISIBILITY
ANALYSIS
ACTION
Cloud
On Premises
PACKETS
LOGS
ENDPOINT
NETFLOW
Intelligence &
Context Tagging
Enrich
User
Behavior
Analytics
Real-Time
Detection
Archiving
Incident
Orchestration
AI
RSA
LIVE
Threat Intel | Business Context
Rules | Parsers
Reports | Feeds
Powered by NW Firstwatch, Incident Response, and Engineering, plus NW Community

Netwitness Agentic AI platform

DATA

NETWITNESS SIEM

Logs

Network Data

Endpoint Data

Asset / Identity Context

CTI Data

AGENTIC ENGINE

SOC AI Analyst

- Automated Triage
- Verdict & Scoring – True / False Positive
- Deep investigation & scoping across logs, network, endpoint & UEBA
- Entity mapping & contextual analysis across datasets
- Automated Enrichment
- Timeline reconstruction & standardized mapping

ANALYST IN THE LOOP

Human validation and final decision

OUTPUT

Executive Summary & Verdict Actions

Timeline & Scope

IOCs & Recommended Actions

NETWITNESS

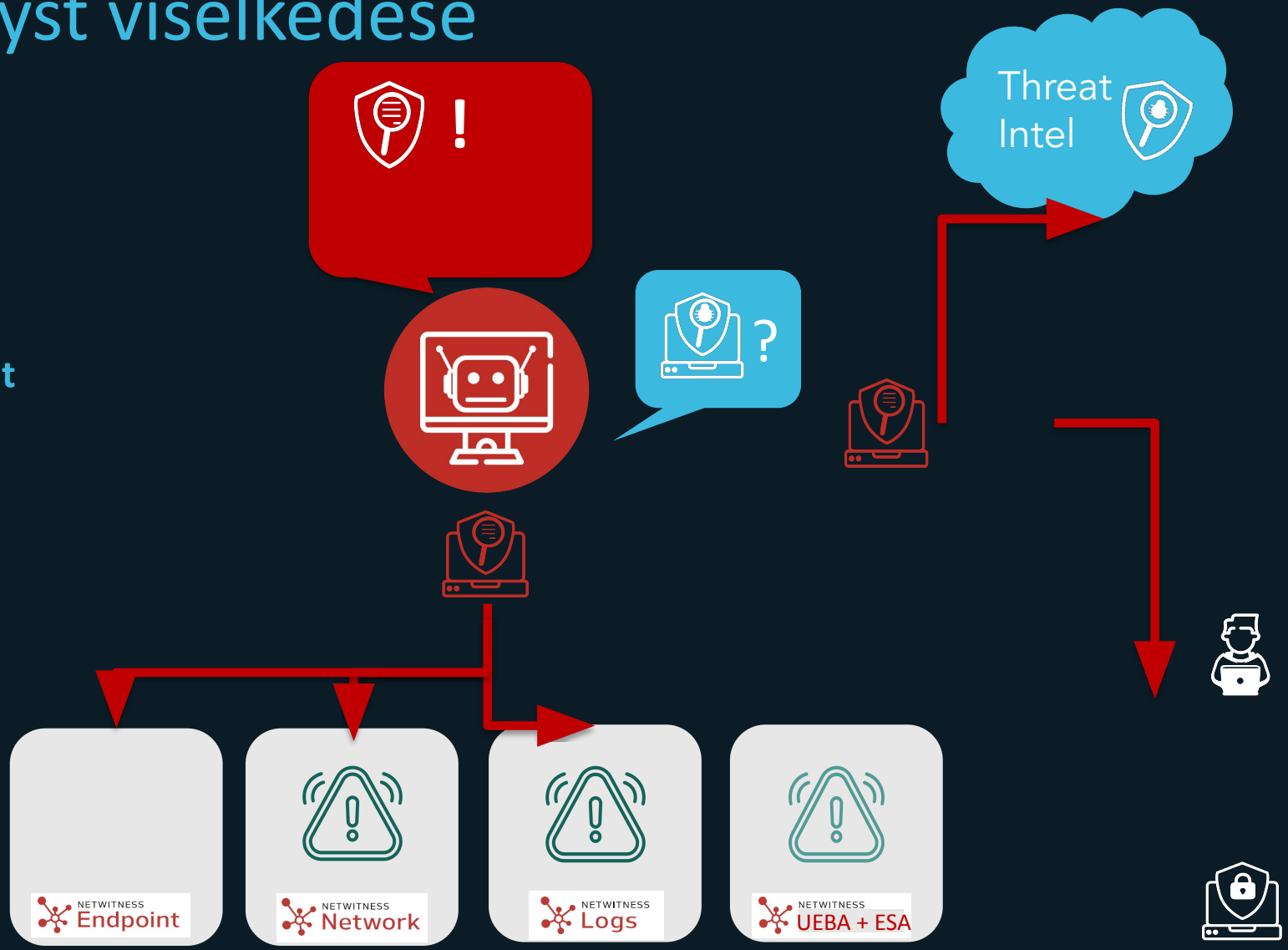
Product Overview

Meet the AI Analyst

2025

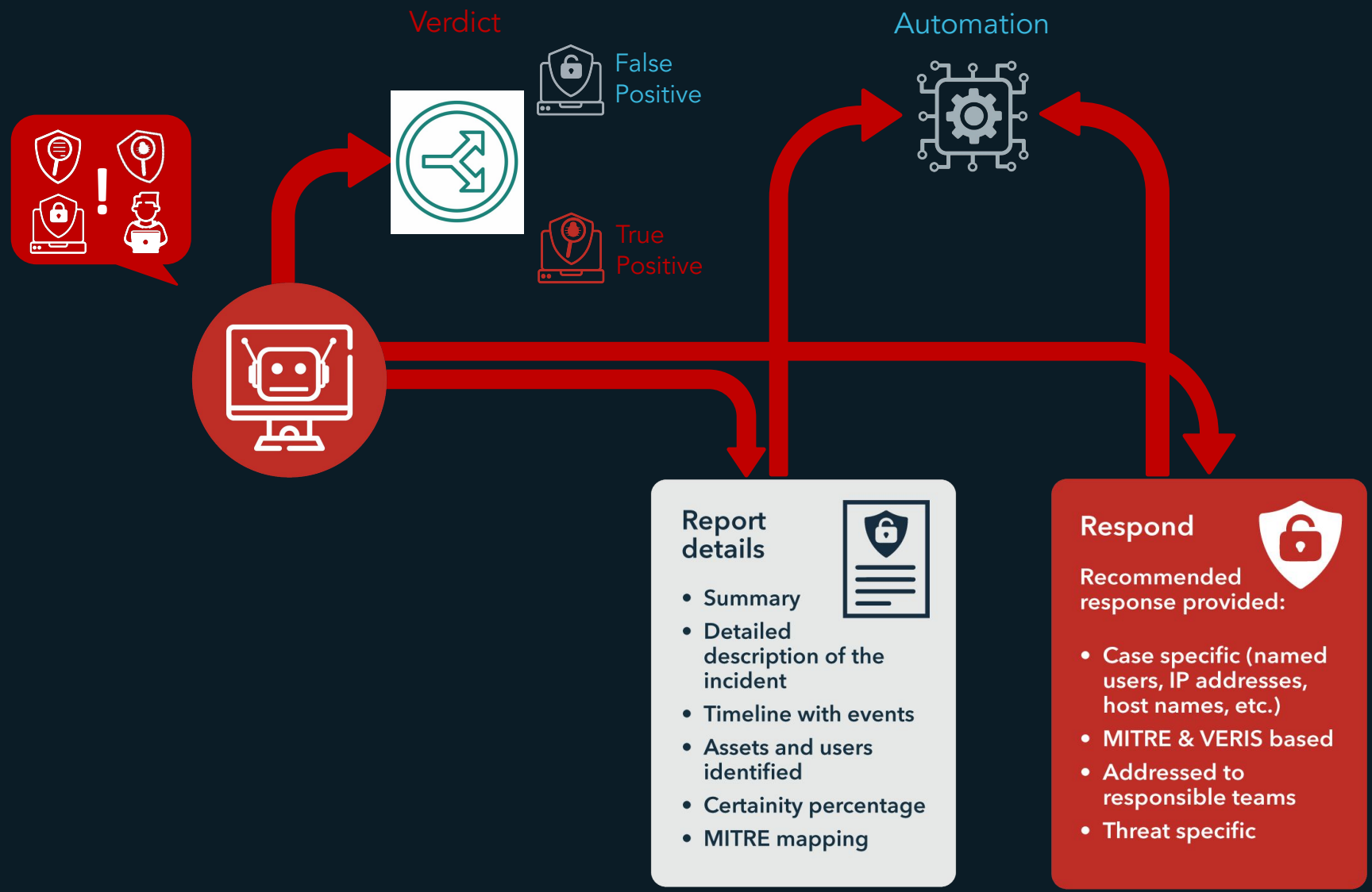
Az AI Analyst viselkedése

Az AI-elemző által támogatott folyamat



Az AI Analyst viselkedése

Triázs, riport,
ajánlott válaszreakciók



AI-támogatott incidenskezelési munkafolyamat

Incidens Észlelés

A rendszer incidenst generál, amely egy potenciális biztonsági eseményt jelez.

AI Agent Vizsgálat és dokumentálás

Az AI mély elemzést végez, majd strukturált jelentést készít.

A jelentés emberi elemzői felülvizsgálata

Egy SOC elemző validálja az AI által generált megállapításokat, biztosítva a pontosságot és a relevanciát.

Döntés (elfogadás vagy felülbírálás)

Az elemző hozza meg a végső döntést arról, hogy az esemény valódi incidens-e, és meghatározza a súlyosságát.

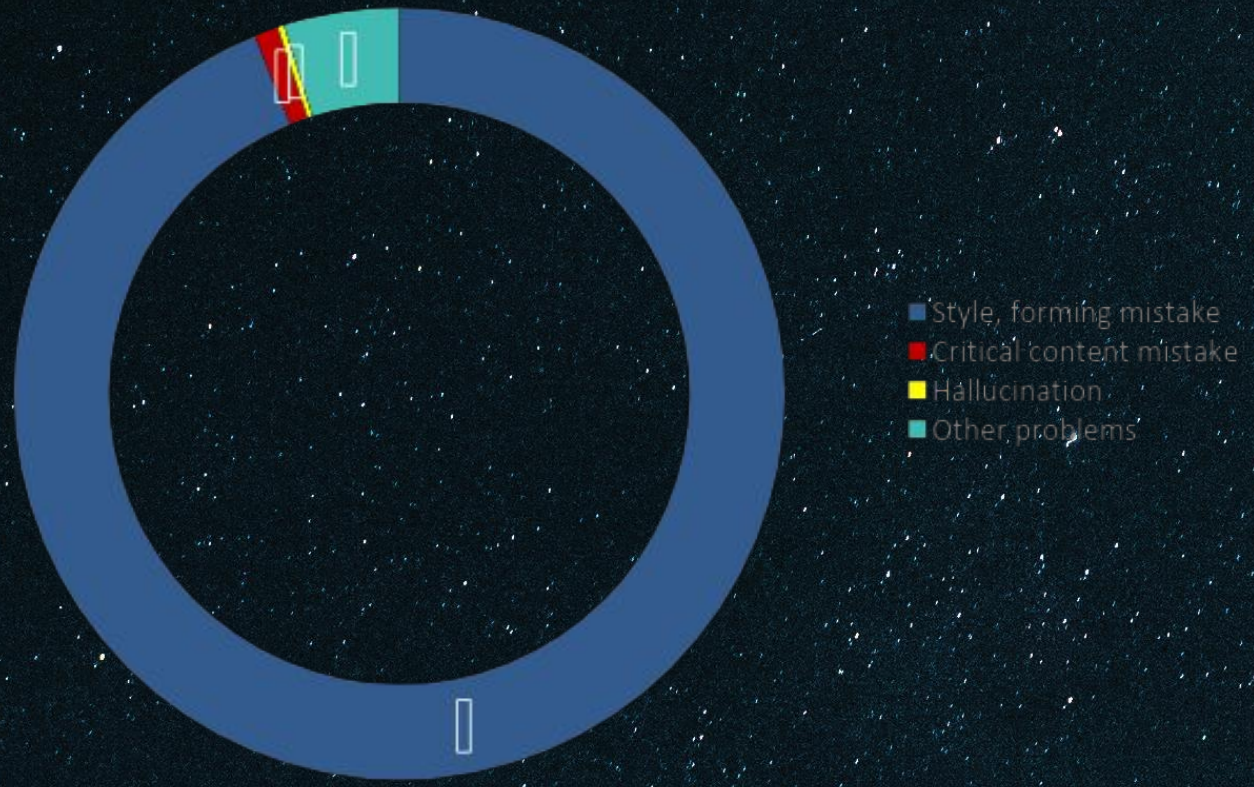
Incidenskezelési intézkedések

A megfelelő playbook végrehajtása vagy manuális válaszlépések elvégzése, például a rendszer izolálása, értesítések kiküldése vagy a hiba elhárítása (remediáció).

Összegzés

8 hónap teszt eredményei: magas pontosság

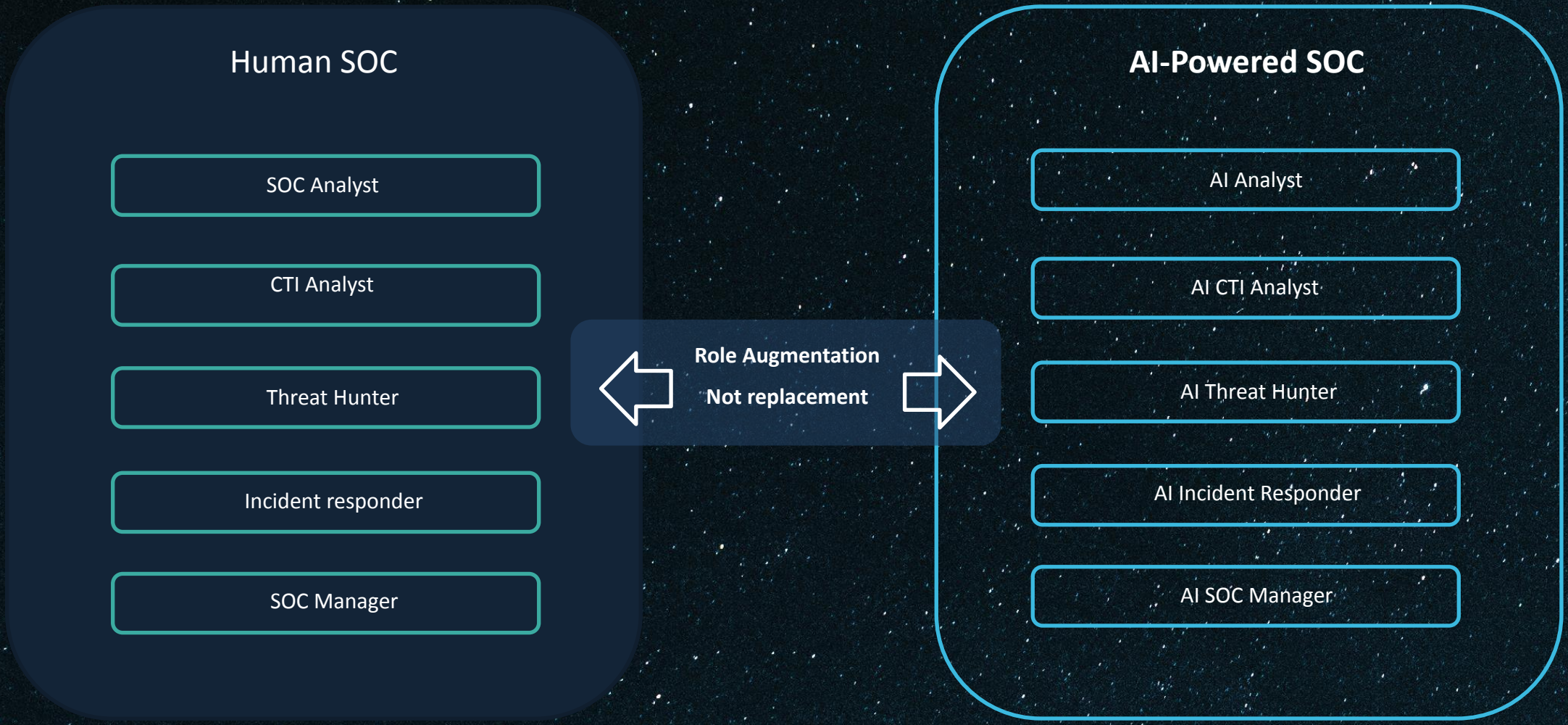
- 93,89% formai probléma
- Kritikus tartalmi hiba: 1%
- Hallucináció (nagyon ritka): 0,27%
- Egyéb problémák: 4,84%
- 62 különböző incidens-típus elemezése:
  - 3 típusnál az AI megengedőbb volt (~4%)
  - 13 típusnál az AI szigorúbb volt (~20%)



Eredmények: 2603 incidens kivizsgálása után

Hagyományos, de fejlett SOC		Agentic AI használatával (Az elemzők 100%-a támogatta a rendszer bevezetését)
20-45 perc	Átlagos incidens várakozási idő	0 perc
15 perc (2,5 perc – 2 óra)	Átlagos humán validálási idő elemzési idő	1,5 perc
70%	Átlagos fals pozitív arány	70%, de az AI mindent kiszűrt!!
minden ügyfélnél létezik ☹	Incidens backlog	MEGSZÜNT ☺
5x8	Átlagos szolgáltatási idő	7x24
20-30 perc	Riport írás időigénye	0 perc

The Agentic SOC Digital Twin



Ügyfél előnyök

Növeli a validált fenyegetések arányát

Biztosítja, hogy az elemzők csak a valós kockázatokkal foglalkozzanak, csökkentve a zajt és a felesleges ráfordítást.

Felgyorsítja a vizsgálatokat és a reagálást

Automatizálja az elemzési lépéseket, lerövidítve az észleléstől a beavatkozásig tartó időt.

Átlátható, megbízható elemzési eredmények

Érthetővé teszi és dokumentálja az eredményeket, így a döntések utólag is visszakövethetők és felülvizsgálhatók.

24/7 folyamatos működés, az emberi elemzői korlátokon

Folyamatos monitorozást és reagálást biztosít fáradtság és leállás nélkül.

Tehermentesíti az elemzőket az ismétlődő, alacsony hozzáadott értékű feladatoktól

Lehetővé teszi, hogy a csapatok a stratégiai fenyegetésvadászatra és a nagyobb értékű biztonsági munkára fókuszáljanak

A NetWitness része, de lehetőség van az integrációra

Gyorsan bevezethető minimális fennakadással, növeli a meglévő eszközök értékét, és más rendszerekhez is integrálható.

Agentic AI - működés közben

2 támadási scenárió

NETWITNESS

Demo attack summary

Case 1: Suspicious IP Detected
Case 2: Suspicious user activity

Case 1 - Suspicious IP Detected

Attack chain explanation I.

Initial Access

- WebServer – RCE vulnerability
- PS-Empire Agent installation (launcher.bat)

Privilege Escalation

- Downloading JuicyNG (ie.exe)
- Gain SYSTEM access

Persistence

- Registry key modification

© 2025 NetWitness LLC. All rights reserved.

Case 1 - Suspicious IP Detected

Attack chain explanation II.

Collection

Lateral movement

Data exfiltration

- Enable WDigest – Registry modification
- Running Mimikatz – Dumping passwords
- Downloading PS-Empire agent to Domain Controller
- Creating scheduled task on Web Server to run Metasploit Agent
- Communication attempt to a „known” malicious IP address via rev_notepad.exe

Case 2 - Suspicious User Activity Incident explanation

New User created

User added to Privileged group

Multiple Failed login attempt

User Lockout

- John Smith user created by Administrator
- John Smith was added to the „Administrators” group by Administrator user
- 10 failed login attempt generated by John Smith
- 10 failed login indicates a user lockout event

Köszönöm a figyelmet

euro one